CYBER TERRORISM AND PUBLIC SUPPORT FOR RETALIATION

A Multi-Country Survey Experiment

British Journal of Political Science

Ryan Shandler [a], Michael L. Gross [a], Sophia Backhaus [b] & Daphna Canetti [a]

[a] University of Haifa, School of Political Science, Israel

[b] University of Oxford, Department of Social Policy and Intervention, United Kingdom

Corresponding Author: ryanshandler@gmail.com

Supplementary materials and replication files available at: sites.google.com/view/ryanshandler

Abstract

Does exposure to cyber terrorism prompt calls for retaliatory military strikes? By what psychological mechanism does it do so? Through a series of controlled, randomized experiments, we exposed respondents (n = 2,028) to television news reports depicting cyber and conventional terror attacks against critical infrastructures in the United States, United Kingdom and Israel. Findings indicate that only *lethal* cyber terrorism triggers strong support for retaliation. Findings also confirm that anger bridges exposure to cyber terrorism and retaliation, rather than psychological mechanisms such as threat perception or anxiety as other studies propose. These findings extend to the cyber realm a recent trend that views anger as a primary mechanism linking exposure to terrorism with militant preferences. With cyber terrorism a mounting international concern, this study demonstrates how exposure to cyber terrorism can generate strong public support for retaliatory policies – depending on the lethality of the terror attack.

Keywords: Cyber-Terrorism; terrorism; retaliation; critical infrastructure; anger.

Introduction

Security officials have long warned of the foreboding threat posed by cyber terrorism. In recent years, following a spate of reports about next-generation cyber attacks causing real-world physical destruction; this threat has come of age. A seminal example was a 2020 cyber attack on a German hospital that led to the death of a patient who had to be hurriedly transferred to another hospital following the devastating attack (Tidy 2020). Several months earlier, Iranian affiliated operatives launched a cyber attack that successfully breached the control systems of Israel's civilian water infrastructure (Heller 2020), while Russian cyber operatives managed to digitally infiltrate power plants across the United States – attaining the ability to remotely control key components of the electricity grid (Sanger 2018). In light of this new cyber reality, scholars have heralded the dawn of 'Kinetic Cyber' – the "credible capability to use cyber attacks to achieve kinetic effects" (Applegate 2013, p. 3).

The scope of the threat posed by this alarming new phenomenon, especially against critical infrastructure, was elucidated most prominently by former CIA Director and U.S. Secretary of Defense, Leon Panetta, when he insisted that the world was "facing the possibility of a 'cyber-Pearl Harbor' [that] could dismantle the nation's power grid, transportation system, financial networks and government (Bumiller and Shanker 2012)". Even as skeptics question what they view as a hyperbolic depiction of this threat (Lawson, 2019; Lewis, 2017; Valeriano & Maness, 2015), there is mounting evidence that terror organizations are adopting cyber tools to launch increasingly sophisticated attacks (Lee et al. forthcoming), and we have witnessed a tenfold increase in significant cyber attacks on critical infrastructure during the last decade (Noguchi and Ueda 2019). Even as debate about the extent of the threat endures, the public continues to exhibit mounting trepidation about the destructive capacity of cyber-terrorism, with recent Gallup polls finding that the American public views cyber-terrorism as the third most critical threat to the U.S. over the next decade – ahead of Chinese military power, conflict in the Middle East or international [conventional] terrorism (Norman, 2018; McCarthy, 2016).

As cyber specialists debate the imminence of a newly physically destructive cyber-terrorism threat, the rise of this phenomenon raises significant new questions for political science that have gone unexplored. How does exposure to cyber terrorism affect political preferences? By what mechanism does it do so? New theories and models relating to cyber terrorism have been developed in the fields of

law (Schmitt 2017), foreign policy and strategic studies (Clarke 2016; Herzog 2011) and psychology (Backhaus et al. 2020; Gross, Canetti and Vashdi 2018), yet equivalent models are conspicuously absent in political science.

To this point in time, an initial body of research has begun to contemplate the political consequences of cyber terror attacks (Hua, Chen and Luo 2018; Gross, Canetti and Vashdi 2016), yet this research is still in its infancy. By contrast, it is well established that exposure to *conventional* terror attacks cause heightened threat perception (Berrebi and Klor 2008; Canetti et al. 2017), anxiety (McDermott and Zimbardo 2007), in-group solidarity and outgroup exclusion (Canetti-Nissim, Ariely and Halperin 2008), and increased demands for government protection and retaliatory policies to defend against future attacks (McDermott and Zimbardo 2007). For now, there is limited evidence whether individuals react to cyber-terror attacks in the same way. It is reasonable to assume that the same outcome of a conventional or cyber terror attack will cause an equivalent reaction in victims. Alternatively, the specter of cyber terrorism may amplify the terror response due to the novelty of the form of attack, the omniscience often associated with cyber operators and uncertainty about the identity of cyber attackers. Still another prospect is that exposure to cyber terrorism may elicit a weaker political response than conventional terrorism due to the lack of historical fatalities associated with cyber attacks. This research responds to the uncertainty by conducting a methodologically rigorous examination of how civilians experience cyber terrorism in its various forms.

Our empirical evidence verifies that cyber terrorism causes distinct political shifts relative to conventional terrorism. We examine the political effects of exposure to cyber terrorism through a series of randomized controlled experiments in three countries - the United States, United Kingdom and Israel. Following two experimental pilots, a culminating experiment exposed 1,848 respondents throughout the three countries to various forms of terror attacks. These controlled experiments test how a) the form of terrorism (conventional kinetic terror vs. cyber terror), and b) the outcome of terrorism (lethal vs. non-lethal effects) influence support for military retaliation. The findings demonstrate that the level of support for retaliatory strikes differs significantly according to the type of terror to which respondents are exposed. Support for retaliatory strikes is substantially lower among participants who viewed cyber terror attacks as opposed to conventional terror attacks, but only when the consequences of the cyber attack are non-lethal. When cyber attacks do cause fatalities, then support for retaliation is just as high as with conventional terror attacks. In this way, we observe a *lethality-threshold* for cyber terrorism effects, wherein the outcome of the attack must meet a minimum level of destructiveness to produce political outcomes at the levels of conventional terrorism. Second, we confirm that the mechanism underpinning the relationship between exposure to cyber terrorism and support for retaliation is driven by a mediated model – whereby exposure to terrorism causes anger, which in turn drives the political support for retaliation. This conclusion extends to the cyber realm recent findings that view anger, and not anxiety or threat perception, as the predominant variable linking political violence and militant attitudes.

Political Consequences of Exposure to Terrorism

Two decades of research have thoroughly identified how exposure to political violence in general, and terrorism in particular, markedly shapes political preferences and behaviors. Moving beyond the early studies that used aggregate-level data to consider the effects of exposure to terrorism, newer studies now integrate the psychological and emotional consequences of exposure into political models that explain particular attitudinal shifts on the individual level. It is established that exposure to conventional terrorism undermines one's sense of security and heightens feelings of vulnerability (Huddy et al. 2005; Neria, DiGrande and Adams 2011; Silver et al. 2002), fosters a threatening worldview and increases support for hardline policies (Bonanno and Jost 2006; Bleich, Gelkopf and Solomon 2003), causes a rightward shift on security and privacy issues (Janoff-Bulman and Usoof-Thowfeek 2009) and leads to increased demands for governments to take strong military action against terror groups (McDermott 2010).

A recurring political effect of interest in the literature is public support for military retaliation against perpetrators. This variable is of interest since scholars have slowly come to agree that public opinion has at least a measurable impact on the decision to engage in sustained military operations, and many IR theories of conflict implicitly incorporate micro-level processes (Kertzer 2017; Klarevas 2002; Foyle 2004; Sobel 2001). Yet the literature offers competing evidence about how exposure to political violence translates into support for retaliation. On the one hand, the fear and anxiety caused by exposure to terror attacks enhance support for precautionary (surveillance) policies, and lower support for military action (Huddy et al. 2005; Lerner et al. 2003). By contrast, exposure to terrorism increases individuals' tendency to vote for right-wing candidates and to engage in risk-seeking behaviors (Berrebi and Klor 2008; Gould and Klor 2010; Jaeger and Paserman 2008; Montalvo 2011). These behaviors are reflected in the tendency to develop more negative out-group sentiments and to intensify demands upon governments to initiate strong military action (Sadler et al. 2005). The differences in exposure effects reflect the multifaceted nature of political policy preferences. A person can simultaneously experience vulnerability and express support for precautionary policies, while at the same time advocate for strong military responses out of a sense of injustice or anger. These ostensibly different findings reflect the particular focus of each study.

The variable of support for retaliation is of particular interest in analyzing the effects of cyber terrorism, since the particular characteristics of cyber terrorism may alter the findings traditionally associated with conventional exposure. One major difference is the difficulty in attribution, which is a characteristic of cyber attacks, and could dampen the effectiveness and attractiveness of retaliatory strikes (Lindsay 2015; Brenner 2006). Jardine and Porter (2020) found that the presence of ambiguity in attributing cyber attacks severely reduces public support for retaliatory options. Kreps and Das (2017) concluded that bipartisan assessments of attribution following cyber attacks can mitigate this lower support, while the consequences of cyber attacks are a key to support for retaliatory airstrikes. Another major difference is that cyber terrorism has not hitherto threatened the physical safety of civilians in the same way as conventional terrorism. The perceived lethality of the terror attack is critical for understanding its impact since most people are threatened by, rather than directly exposed to the terror act, and the perception of lethality is an important factor in its individual-level impact (Getmansky and Zeitzoff 2014). The limited danger of cyber attacks has become a characteristic feature in discussions about the phenomenon, and it would make sense that cyber terrorism is experienced and perceived differently than other forms of terror acts that bear the possibility and even likelihood of fatal consequences. Finally, in the face of historical terror attacks, civilians could seek safety in their homes, bomb shelters or in other countries to attain a sense of security. None of these assumptions hold true for cyber terrorism where an unidentified perpetrator can break into any digitally connected device irrespective of geographic proximity.

The important factor in examining the public response to terror attacks is not the objective analysis of substantive differences between cyber terrorism and conventional terrorism, but the manner in which they are subjectively perceived by citizens who are exposed to attacks. Research by Tomz and Weeks (2016) and Kreps and Schneider (2019) found that the public is loath to escalate aggressively in response to cyber attacks, even when if the effect is equivalent to conventional attacks. Their research theorized that individuals experience cognitive dissonance following exposure to cyber attacks since the natural inclination for vengeance is counteracted by the virtual qualities of the cyber sphere that are associated with lower threat. Our research builds on these foundational studies by concentrating our focus on cyber terrorism in particular, rather than cyber attacks generally. This focus on cyber terrorism is especially important seeing as the primary threat of exposure to destructive cyber attacks is via terrorism (Albahar 2019), and the response to an external threat cannot be separated from the conceptualization of the attacker. Under this terror-centric framework, we propose to take into account a number of competing variables including the nature of the attack (cyber means versus conventional [kinetic] means), as well as the lethality of the attack. We advance the following two hypotheses: (H_1) People who are exposed to cyber terrorism will demand retaliation at lower levels than people exposed to kinetic terrorism; and (H_2) People who are exposed to fatal terrorism will demand retaliation at

higher levels than people who are exposed to non-fatal terrorism – regardless of the form of attacks (cyber vs. conventional).

Theorizing Anger as a Mechanism

Anger is "an emotional state that consists of feelings that vary in intensity, from mild irritation or annoyance to intense fury and rage" (Spielberger et al. 1995). The underlying drive of the anger emotion is often defined as a desire to correct perceived injustice or unfairness (Fischer and Roseman 2007, Halperin et al. 2011). Cyber and conventional terror attacks that directly transgress norms regarding the use of force are especially likely to evoke anger and a desire for retaliatory strikes – even if the threat was not experienced on a personal level.

The theory of emotionally driven foreign policy preferences in the aftermath of political violence is well established. In the aftermath of conventional terror attacks, we know that a variety of negative emotions (anger, rage, sadness, etc.) enhance support for aggressive foreign policy responses (Kupatadze and Zeitzoff 2019; Small, Lerner and Fischhoff 2006; Lerner et al. 2003). Yet how does this mechanism translate to the phenomenon of cyber terrorism specifically? It could be that cyber terrorism will cause high levels of emotional responses due to the novelty of the cyber form of the terrorism, lower levels due to low subjective predictions of the likelihood of harm, or the same level of anxiety due to a lack of perceived distinction between cyber and conventional terror.

Experimental research has identified causal pathways between exposure to terrorism and political outcomes with various intervening emotional variables such as fear and anxiety (Huddy et al. 2005; Lerner et al. 2003; Skitka et al. 2006), threat perception (Wayne 2019; Kupatadze and Zeitzoff 2019; Stevens and Vaughan-Williams 2014; Huddy et al. 2002), and sadness (Nussio 2020). While fear and anxiety are a common response to exposure to terrorism, this does not always translate to heightened support for military retaliation or other corrective political acts, since fear is elicitied primarily by attacks that are personally experienced (Huddy et al. 2005; Haidt et al. 2003). Likewise, the literature suggests that the intervening effect of threat perception is minimized in cases of limited information, such as with cyber terrorism (Egloff 2020). However most recent research has identified that "*the dominant response of civilian populations to terror threat is not fear and a desire to reduce future personal risk, but rather anger and a desire for vengeance*" (Wayne 2019, p. 5). Exposure to terror events is typically and understandably accompanied by anger (Carver 2004; Hirsch-Hoefler et al. 2016; Lerner et al. 2003; Steele, Parker and Lickel 2014). In the case of terrorism especially, anger is more likely to intervene in any retaliation-centric mechanism since it is linked to more superficial and heuristic-based cognitive processing that is associated with aggressive policy options (Bodenhausen, Sheppard and Kramer 1994; Sirin and Geva 2013). Indeed, one recent multi-country study found that only those respondents who expressed anger following exposure to a terrorist threat become more supportive of drone strikes against terrorists (Fisk, Merolla and Ramos 2019).

This literature poses a conceptual dilemma in applying its conclusions to the phenomenon of cyber terrorism due to the absence of physically present perpetrators and the difficulty of attributing attacks to a source. Anger is typically associated with wielding a sense of control, yet this raises questions about how people express their anger in cases where the perpetrator is unknown – a common occurrence in the cyber realm. Cyber terrorism is certainly more nebulous, abstract, and difficult to connect the cause and effect compared to conventional terrorism, where there's visceral and direct evidence of the attack. Nonetheless, we assert that anger maintains its potency in regulating foreign policy preferences in these situations for the following reasons. A persuasive line of research has identified how anger can lead to a generalized desire for revenge and retribution – even when there is uncertainty as to the identity of the attacker, or when the target is symbolically similar to the perpetrator (Liberman and Skitka 2019; 2017; Washburn and Skitka 2015). These findings draw on social psychological theories to demonstrate the political equivalent of "displaced aggression" – a tendency to express heightened support for aggressive action towards tangentially related third parties in the aftermath of attacks. Essentially, this theory demonstrates that anger can lead to a general

increase in punitive inclinations, and that the anger needn't be directed against a specific target in order to heighten support for retaliation. This vicarious retribution theory is especially useful in analyzing exposure to cyber-terrorism where the identity of the attack is often unknown or uncertain. The theory explains how the experience of anger translates to heightened general punitive impulses against unrelated offenders (Liberman and Skitka 2019) or symbolically similar outgroups to whom responsibility is imputed (Liberman and Skitka 2017; Washburn and Skitka 2015).

We assert that weighing these factors, the political effects of exposure to cyber terrorism are most closely related to the anger emotion and its association with aggressive policy preferences. Following this pathway, we hypothesize that (H_3) *preferences for retaliatory strikes following cyber and conventional terror alike will be mediated by the emotion of anger, and not by the emotion of anxiety or a sense of perceived threat.*

A Three-Country Survey-Experiment

To test these hypotheses, we ran a series of controlled randomized survey-experiments that simulated television news reports about different forms of terror attacks in the United States, United Kingdom and Israel. The experimental manipulation relied on professionally produced original video clips that broadcast breaking news reports showing various forms of terror attacks on railway infrastructure. Experiments in recent years have shown how exposure to broadcast videos and media reports of terror attacks are sufficient to cause shifts in levels of anxiety, anger and political attitudes (Shoshani and Slone 2008; Backhaus, 2020). We further believe that high quality, professionally produced television news reports are more ecologically valid and authentic than comparatively sterile vignettes that seem to be the norm in many survey experiments regarding terrorism and political violence. To further substantiate this belief, we ran a pilot experiment (n = 180) that affirmed that exposure to breaking news media reports depicting terror attacks against train networks causes substantial variance in emotional and political responses depending on the type of terror attack. (The analyses and media reports for this pilot dataset appear in Online Appendix A).

We randomly assigned respondents (n = 1,848 among the three countries) to one of five conditions in a 2X2 experimental design with a control group. The conditions included: *Lethal Cyber Terrorism Condition* - a cyber terror attack by an as yet unidentified perpetrator caused a train to derail causing the deaths of 7 passengers and causing critical injury to another 10 passengers. Lethal *Conventional Terrorism Condition* - the same outcome was caused by a conventional terror attack. Non-Lethal *Cyber Terrorism Condition* - a cyber terror attack by an as yet unidentified perpetrator targeted a railway leading to the theft of tens of millions of dollars from passengers' credit cards. Non-Lethal *Conventional Terrorism Condition* - the same non-fatal outcome was perpetrated using conventional terror means. A fifth control condition did not utilize any news stories or refer to the train system in any way. The experiment therefore manipulates forms of terror attacks on two axes: the type of attack (cyber vs. conventional) and the consequences of the attack (lethal vs. financial). (See Table 1 for an overview of the conditions, and Online Appendix B for a complete script and screenshots). The news clips purported to broadcast on local news stations in the three countries - NBC News in the United States, Sky News in the United Kingdom and Channel 2 in Israel. The clip and news story was identical in each country, adapted only to refer to local cities and railway companies, and with the relevant introductory special alert animation and logo of the broadcaster. Every other element remained identical - including the news presenter. In line with the analysis conducted by Jarvis, Macdonald and Whiting (2017), we abided by the principle of specificity in producing the news reports, a feature that is associated with accuracy and with eliciting high levels of concern in cyber terrorism reporting. The script was translated and back translated.

Table 1. Description of treatment conditions

Treatment Condition	Method of attack	Consequences of attack	Screenshot from Breaking News Report
Lethal cyber terrorism	Cyber attack	The attack caused a train to derail causing the deaths of 7 passengers and causing injuries to an additional 10 passengers	
Non-lethal cyber terrorism	Cyber attack	The attack targeted railway headquarters leading to the theft of tens of millions of dollars from passengers' credit cards.	
Lethal conventional terrorism	Conventional attack	The attack caused a train to derail causing the deaths of 7 passengers and causing injuries to an additional 10 passengers	
Non-lethal conventional terrorism	Conventional attack	The attack targeted railway headquarters leading to the theft of tens of millions of dollars from passengers' credit cards.	
Control	N/A	Did not view any video	Did not view any video

Screenshots are taken from the UK news reports.

The news clips purported to broadcast on local news stations in the three countries - NBC News in the United States, Sky News in the United Kingdom and Channel 2 in Israel. These outlets were selected due to their standing as nationally syndicated news outlets, with among the highest and most bipartisan levels of public trust. (Although it may be more accurate to describe them as possessing the least lousy levels of public trust). NBC News, for example, is one of only three nationally broadcast television news sources that are trusted by more than 30% of both Republicans and Democrats (Pew Research Center 2020). Sky News, likewise, is ranked as one of the three most trusted UK news brands (Nielsen, Schulz and Fletcher 2020). Unlike the BBC, for example, which has significant variance in trust levels according to political identity, Sky News possesses highly consistent views among the full ideological spectrum (Nielsen, Schulz and Fletcher 2020). In Israel, being a smaller media market, there is less scholarship on public trust in the various media outlets. Yet Channel 2, before it was split into competing broadcasters, was the largest and most authoritative news source with an audience share of above 20% - double the next highest national news network (Dorot 2020)

While acknowledging the thriving literature on partisanship in the ascription of trustworthiness in media outlets, we note that this methodology abides by the highest levels of ecological validity in that the public is exposed to terror attacks via news reports that are not devoid of preconceived notions of credibility. We contend with this challenge by controlling for relevant variables that influence trust (political identity, age, etc.) and we also work to minimize these effects by abiding by the principle of specificity in producing the news reports, a feature that is associated with accuracy and with eliciting high levels of concern in cyber terrorism reporting (Jarvis, Macdonald and Whiting 2017). We are further comforted by prior empirical research emphasizing the fact that the professionalism and expertise in the production of television news segment is a more significant factor in imputing credibility and emotional resonance than the broadcaster label (Tewksbury, Jensen and Coe 2011). The script was translated and back translated to ensure for cross-language consistency.

After viewing the video treatment, respondents completed a detailed questionnaire exploring their emotional state, political attitudes and demographic information. The dependent variable of interest in this study was support for retaliation policies. Support for retaliation was measured using an adapted six-item summative index from Graves, Acquisti and Anderson (2014). Respondents were asked to indicate their support for various military and diplomatic responses to attacks on the soil of their respective countries. Retaliatory options included cyber and conventional military attacks on military and civilian targets, economic sanctions and diplomatic maneuvers. (For example – to what extent do you support missile strikes against military targets of the attacker; to what extent do you support freezing the attackers' bank accounts and imposing economic sanctions?) All questions were rated on a scale of 1 (not at all) to 6 (absolutely), and post-hoc analysis showed the scale to be highly reliable (Cronbach's $\alpha = .80$).

Anger, the hypothesized mediating variable, was measured with the shortened version of the commonly used STAXI measure (State-Trait Anger Expression Inventory; Spielberger 1988), comprised of 4 items that assess the intensity of anger as an emotional state at a particular moment in time. Respondents rated items on a scale of 1 – 6 (1 = not at all; 6 = absolutely). The inventory is scored as the total mean of all items, with higher scores reflecting higher levels of state anger (Cronbach's $\alpha = .96$).

Anxiety was measured using the short form Spielberger state-anxiety inventory-6 (Marteau and Bekker 1992; Spielberger 1970). This commonly used six-item index measures both state (extrinsic) and trait (intrinsic) anxiety. Respondents were asked to rate on a scale of 1–6 (1 = not at all; 6 = absolutely) the extent to which their feelings 'at the moment' correspond to different items. Half of the items represent negative feelings and emotions (e.g. 'I feel upset', 'I feel worried) and the other half represent positive feelings and emotions (e.g. 'I feel relaxed', 'I feel content) (Cronbach's $\alpha = .88$).

In accordance with standard methodological practices, and to avoid the pitfalls of confound and unseen interaction effects, the dependent variable measures were placed in the survey immediately after respondents were exposed to the experimental treatment. Other covariates collected included age, gender, level of education, political self-identification, family income, average daily Internet usage,

computer literacy and usage of public transportation. All demographic covariates were collected at the end of the survey.

Participants and Countries

The questionnaires were distributed simultaneously in the three countries between October 14, 2018 and October 17, 2018. The survey was distributed using three Internet survey platforms - Amazon Turk, Prolific and Midgam - in the US, UK and Israel respectively. (See Online Appendix C for a discussion of the advantages and shortcomings of the selected survey panels). At the outset of the surveys, respondents were told that they were to view an authentic video news story and answer several questions. In line with restraints imposed by the IRB board, respondents diagnosed with PTSD symptoms or having experienced trauma during the preceding two years were excluded from participating in the survey. An attention check was conducted following the video manipulation leading to the exclusion of 16 respondents (0.8% of the total). During the debriefing, we communicated to the respondents that the videos were scripted and did not reflect real-world events.

The study participants represented a cross study of the general adult population in each country US: (N=607, Mage= 37 years, SD =10.31); UK: N=597, Mage= 37 years, SD = 11.93) and Israel, (N=644, Mage = 39, SD = 13.16). The distribution of the political orientation of the sample in Israel skewed more right wing than the US and UK, and the UK sample had a higher portion of female respondents than the US and Israel. Online Appendix D presents the detailed statistics of the sample and balance checks across the conditions.

We chose to focus on the United States, United Kingdom and Israel since they share several features in common. First, each of these countries is among the short list of states that have been exposed to publicly reported cyber attacks on critical infrastructure. Second, each of these three countries is ranked within the same decile in terms of the social and economic impact of terrorism as measured by the Global Terrorism Index. Third, each of the countries has high levels of Internet penetration and publicly renowned levels of cyber-security preparedness to deal with cyber attacks on critical infrastructure. While the quality of the past terrorism exposure is likely to be different (Israel is exposed to more persistent and repeated terror attacks, while in the US and UK there have been fewer yet larger attacks), all three register high levels of perceived threat from terrorism. The full comparative data appears in Table 2. The selection of these countries additionally reflects a reality whereby the countries currently most susceptible to cyber-terror attacks are the United States, Europe and the West more broadly (Macdonald, Jarvis and Lavis 2019). This western-centric emphasis is explained by the disproportionately heavy reliance on digital systems that accompanies economic development, as well as the natural tendency of terrorism to be exercised in asymmetric conflicts against more conventionally powerful states (Macdonald, Jarvis and Lavis 2019). We note, however, that new research has revealed a growing trend of cyber-terror attacks targeting developing countries in the Middle East, Africa and South America as the threshold to gaining destructive cyber tools becomes gradually lower (Lee et al. forthcoming).

Table 2 – Comparative Analyses of Factors Relevant to Cyber Terrorism Exposure in the United States, United Kingdom and Israel

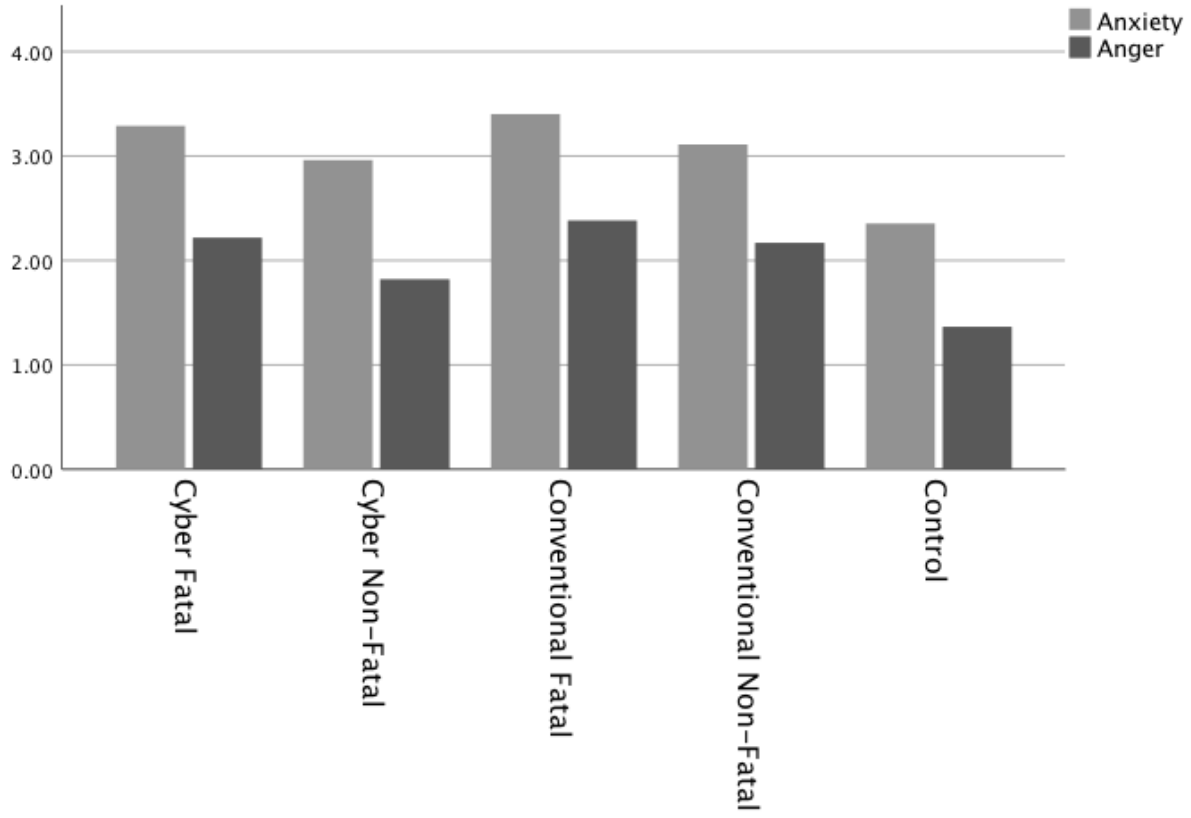
	United States	United Kingdom	Israel
Global Terrorism Index Ranking (impact of terrorism on country) [a]	Ranked 32 of 130 countries	Ranked 35 of 130 countries	Ranked 36 of 130 countries
Ranking of cyber security preparedness to deal with cyber attacks on critical infrastructure [b]	1 (highest) out of 195 countries	5 out of 195 countries	6 out of 195 countries
Percentage of population fearing that a major terror event will take place [c]	51%	65%	70%
Reported instances of cyber attacks on critical infrastructure [d]	14	2	1

Sources: ([a] Institute for Economics & Peace 2017; [b] Shafqat and Masood 2016; [c] Bulman 2018; Israel Democracy Institute 2016; [d] Critifence 2018;)

Main Results

A preliminary step of our analysis strategy was to verify the emotional effects of exposure to the various terror conditions. This has the benefit of testing the efficacy of the experimental manipulation by confirming differential responses among the different conditions. We tested this by running two one-way analyses of variances tests with the type of terror attack as the independent variable and anxiety and anger as the respective dependent variables. The results (see Figure 1) reveal clear differences among the conditions for both anxiety ($F(4, 1,827) = 48.459$, $p<.000$) and anger ($F(4, 1,827) = 37.113$, $p<.000$). Post-hoc analysis using the Tukey HST statistic revealed that for both anxiety and anger, each of the four terrorism exposure conditions reported statistically significantly higher levels of anxiety and anger than the control condition at the .000 significance level for each data point. This result held when looking at the combined sample (n=1,832) and at each individual country sample alone.

Figure 1: Levels of Anxiety and Anger by Exposure to Terror Conditions



The next step of our analysis strategy was to explore any variance in the political effects of exposure to the distinctive terror conditions. Our dependent variable is support for retaliatory strikes against the perpetrator of a terror attack. As described above, this variable was measured using multi-item summative scales with high internal validity. After conducting an exploratory factor analysis, we removed two items from the six-point retaliation measure, which distinguished between military strikes and diplomatic retaliatory responses. The final scale comprises of four items asking about cyber strikes or missile strikes against military or civilian targets. Table 3 summarizes the mean scores for each of the variables of interest showing how each country responded to the various terror conditions to which they were exposed.

Table 3 – Means for Participants on Political and Emotional Measures

Country	Treatment Condition	N	Support for Retaliatory Strikes	Level of Anxiety	Level of Anger
United States	Cyber Terror - Fatal	118	3.24	3.43	2.71
	Cyber Terror – Non-Fatal	119	2.95	2.98	1.90
	Conventional Terror - Fatal	119	3.21	3.55	2.68
	Conventional Terror – Non Fatal	116	3.07	3.10	2.30
	Control	125	3.45	2.21	1.54
United Kingdom	Cyber Terror - Fatal	120	2.55	3.31	2.04
	Cyber Terror – Non-Fatal	119	2.40	2.90	1.68
	Conventional Terror - Fatal	118	2.80	3.44	2.32
	Conventional Terror – Non Fatal	120	2.53	3.22	2.09
	Control	120	2.61	2.39	1.23
Israel	Cyber Terror - Fatal	125	3.98	3.14	1.93
	Cyber Terror – Non-Fatal	130	3.64	2.99	1.88
	Conventional Terror - Fatal	122	4.23	3.22	2.16
	Conventional Terror – Non Fatal	123	4.07	2.79	1.86
	Control	138	4.23	2.45	1.32
Combined countries	Cyber Terror - Fatal	363	3.26	3.29	2.21
	Cyber Terror – Non-Fatal	368	3.02	2.96	1.82
	Conventional Terror - Fatal	359	3.42	3.40	2.38
	Conventional Terror – Non Fatal	359	3.23	3.11	2.17
	Control	383	3.33	2.35	1.36

Note: All measures operate with a scale from 1 – 6 where 1 represents the lowest and 6 represents the highest score.

To test how exposure to terror affects support for retaliatory strikes, we ran a series of OLS regression analyses (see table 4). The four models show the collective and country-level effects of each experimental terror condition as compared to the *conventional fatal terrorism* group, which acts as the reference condition. We elect to use this subset as the reference condition since lethal conventional terrorism is the classic and emblematic form of terrorism against which we are comparing the new form of cyber terrorism in all of its guises. Moreover, this form of terrorism elicited the highest levels of demand for retaliation, allowing us to easily observe the extent to which the other forms of terrorism lowered the demand for retaliatory strikes. What starkly emerges when comparing the different terror types is that the strongest effect materializes in the cyber non-fatal terror condition, which predicted the lowest support for retaliation (approximately 0.4 scale points lower than the control group; $p = .000$). This effect raises the notion that cyber attacks may require a physically destructive element to trigger emotional responses akin to other terror responses. The effects hold while controlling for basic demographic variables and other related variables such as previous exposure to terror incidents, and regular use of public transportation. Of the control variables that we incorporated, two in particular possessed a strong effect on retaliatory preferences. Firstly, as would be expected, political orientation is a key predictor of support for retaliation. For every one scale point rightward on a 1-7 scale of political attitudes where seven is the most right-wing, respondents exhibit higher support for at between .2 and .3 scale points on a 7 point scale. This effect is significant at the .000 level among all countries and in the collective sample. Likewise, gender has a uniformly predictive effect in our model, with men more likely to support retaliation against terror groups in all models. Breaking down these findings by country reveals that the combined effects are driven primarily by the Israeli and United Kingdom samples, with the United States showing no variance in retaliatory preferences compared to the control group.

Table 4. OLS regression models of support for retaliation policies – individual terror conditions

	(1) Three Countries	(2) U.S.	(3) U.K.	(4) Israel
Cyber Terror (Fatal) Condition – Dummy Variable	-.153 [.079]	.045 [.773]	-.281 [.054]	-.278 [.059]
Cyber Terror (Non-Fatal) Condition – Dummy Variable	-.393*** [.000]	-.179 [.249]	-.355* [.016]	-.626*** [.000]
Conventional Terror (Non-Fatal) Condition – Dummy Variable	-.172* [.048]	-.077 [.622]	-.235 [.107]	-.209 [.159]
Control Condition – Dummy Variable	.031 [.713]	.264 [.086]	-.157 [.279]	-.001 [.995]
Political Orientation (1 = very left wing, 7 = very right wing)	.245*** [.000]	.218*** [.000]	.211*** [.000]	.294*** [.000]
Age	.000 [.618]	-.004 [.429]	-.005 [.205]	.000 [.578]
Gender (0 = male; 1 = female)	-.384*** [.000]	-.246* [.016]	-.517*** [.000]	-.365*** [.000]
Previous Exposure to Terror Attacks (0 = no exposure, 1 = exposure)	.096 [.081]	-.020 [.840]	.044 [.635]	.244** [.008]
Regular User of Public Transportation (0 = no or low use, 1 = regular use)	.198*** [.001]	.612*** [.000]	-.037 [.719]	.069 [.474]
Parental Status (0 = no children, 1 = children)	.294*** [.000]	.384*** [.000]	.197 [.062]	.131 [.193]
Country Dummies	Yes	No	No	No
Observations	1,832	597	598	638
R-Squared	.309	.215	.134	.166
Adjusted R-Squared	.304	.201	.119	.153

Note: regression coefficients with p-values in brackets.

** $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$*

Two additional sets of regression analyses further substantiate the difference between the cyber and non-cyber, and fatal and non-fatal forms of terror attacks (see Table 5). We first combined the two cyber terror conditions into one group and the two conventional terror conditions into another group – ignoring the fatality of the strikes and focusing purely on the form of the terror attack. In this analysis, conventional terrorism it the reference group, against which the effects of exposure to cyber-terrorism is compared. (Table 5, Model 1). In the second analysis, we combined the two fatal terror conditions and the two non-fatal terror conditions into separate groups – disregarding the form of the terror attack and focusing purely on its consequences. In this analysis, fatal terrorism it the reference group, against which the effects of exposure to non-fatal terrorism is compared. (Table 5, Model 2). We then ran the same regression analyses testing the effect on retaliation preferences while controlling for the same covariates as above. These analyses reveal a number of interesting facts. First, when focusing only on the type of terror attack and putting the consequences to the side, we can see that respondents exposed to cyber terror attacks were significantly less likely to demand retaliation than respondents exposed to conventional terror attacks. Second, when concentrating only on the consequences of terror attacks, we can see an equally strong effect wherein non-fatal attacks are considerably less likely to evoke strong demands for retaliation than fatal attacks. This supports hypothesis 2 that suggested that the fatality of a terror attack will be a significant predictor of support for retaliatory strikes. These finding additionally illuminate the negligible effect of non-fatal cyber-terrorism depicted in table 4 –

seeing as this form of terrorism appears to suffer from two deficits, lacking both conventional form as well as lethal outcome.

Table 5. OLS regression models of support for retaliation policies – grouped terror conditions

		(1)	(2)
Predictor Variables ↓	Reference Condition →	Conventional (Kinetic) Terrorism	Fatal Terrorism
Cyber Terror Conditions – Dummy Variable		-.187** [.002]	---
Control Condition – Dummy Variable		.118 [.111]	.108 [.143]
Fatal Terror Conditions – Dummy Variable		---	-.208*** [.001]
Demographic variables as appearing in table 3		Yes	Yes
Country Dummies		Yes	Yes
Observations		1,832	1,832
R-Squared		.304	.305
Adjusted R-Squared		.300	.301

Note: regression coefficients with p-values in brackets.
* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

We note an unanticipated finding - that the control (reference) group exhibited an equally high level of support for retaliation when compared to the conventional terrorism condition and the fatal terrorism condition. This is explained by the fact that control group respondents, who did not view any video, were asked to indicate their support for military strikes in response to an unviewed attack – a fact that evoked the worst possible scenario (i.e. a high casualty terror attack). We ran a post-hoc experiment to test this theory with a new dataset (N=737 respondents among all three countries) and found that respondents in the control group did indeed envision a high casualty terror incident – akin to the conventional fatal terror group. The full analysis of this post-hoc evidence appears in Online Appendix E.

Anger Mechanism Estimation

We hypothesized that increased levels of anger would mediate and explains a substantial portion of the relationship between exposure to cyber and conventional terrorism with retaliation preferences. This is based on the theory that the dominant response of civilian populations to terror threats anger and a desire for vengeance (Fisk, Merolla and Ramos 2019; Wayne 2019). This anger-driven mechanism can be reflected in a basic mediation model explaining attitudes towards retaliatory strikes following terror attacks. In this case T reflects exposure to a terror attack; Y is the level of support for retaliatory strikes; and M is the anger caused by exposure to the terror attack – the mediator variable. Our expectation is that it is not the mere fact of exposure that causes a demand for retaliation, but rather that exposure leads to anger, which in turn makes respondents more likely to support retaliatory strikes.

To estimate this mediation effect, we employ the accepted technique developed by Imai, Keele, Tingley, and Yamamoto (Imai et al. 2011). This technique requires that we estimate two equations and then perform a bootstrap simulation.

$$M_i = \alpha_1 + \lambda_1 T_i + x\beta + \epsilon_i \quad (1)$$

$$Y_i = \alpha_2 + \lambda_2 T_i + \gamma M_i + x\beta + \epsilon_i \quad (2)$$

Each equation runs a least-squares regression, appearing in table 6. The left-hand side (dependent) variable is the anger variable in equation (1) (M), and support for retaliatory strikes in equation 2 (Y). The right-hand side contains the exposure to terrorism variable (T) plus a vector of control variables (x) that were collected before the treatment was administered. Equation (2) also includes the mediating anger variable. Having calculated the coefficients and standard errors from these two equations, the Imai procedure then computes the average causal mediation effect (ACME), which is the estimate of the effect that the exposure to terror treatment (T) exerted on support for retaliation (Y) through the mediator variable (M). Due to the weakness of this procedure in integrating multicategorical independent variables, we convert the exposure to terror variable into a binary paradigm and run the analysis twice. The first analysis equates exposure to cyber terrorism as 1 and the control group as 0. The second analysis equates exposure to conventional terrorism as 1 and the control group as 0. Further information on meeting the sequential ignorability assumption required to effectively estimate the true mediation effect appears in Online Appendix F.

Table 6 reports the findings of two mediation analyses on the experimental data, with the main parameters of interest shaded in grey. Each of the different conditions needed to prove a mediation effect is present. First, both treatment effects (exposure to cyber or conventional terror) have a positive effect on the anger variable, as captured by the shaded coefficients appearing in columns 1.1 and 2.1. The second condition is that the anger mediator exerts an effect on the dependent variable, a fact that is shown in the shaded coefficients appearing in columns 1.2 and 2.2. In both cases, the anger variable is a strong predictor of support for retaliatory strikes. The final and most important condition is that the ACME is nonzero. The shaded figure at the bottom of the table indicates that the causal mediation effect is .100 (p = .000) and .109 (p = .000) respectively. Contrasting these figures to the total effects, we can see that a substantial portion of the increased support for retaliatory strikes following cyber and conventional terror strikes is due to the anger evoked by the strike.

Table 6. Mediation Regression Results

Independent Binary T Variable:	1. Exposure to Cyber Terrorism vs. Control Group		2. Exposure to Conventional Terrorism vs. Control Group	
Variable Model →	Equation (1) (Mi) 1.1	Equation (2) (Yi) 1.2	Equation (1) (Mi) 2.1	Equation (2) (Yi) 2.2
Anger		.153 *** (.030)		.120 *** (.028)
Exposure to Type of Terror Attack (T Variable)	.658 *** (.073)	-.410 *** (.076)	.910 *** (.078)	-.225 ** (.078)
Country = United States (dummy variable)	.441 *** (.087)	-.696 *** (.089)	.610 *** (.094)	-.804 *** (.090)
Country = England (dummy variable)	.093 (.090)	-1.107 *** (.091)	.249 ** (.097)	-1.176 *** (.091)
Political Orientation	.111 *** (.023)	.218 *** (.023)	.139 *** (.025)	.255 *** (.024)
Age	.000 (.000)	.000 (.000)	.000 (.000)	.000 (.000)
Gender	-.043 (.070)	-.255 *** (.070)	.091 (.076)	-.431 *** (.072)
Constant	1.268 *** (.394)	3.467 *** (.399)	.993 * (.480)	3.460 *** (.452)
ACME (95% confidence interval)	.100 *** [.052, .15]		.109 *** [.056, .17]	
Direct Effect (95% confidence interval)	-.410 *** [-.558, -.26]		-.225 *** [-.382, -.08]	
Total Effect (95% confidence interval)	-.309 ** [-.455, -.16]		-.115 [-.258, .02]	
N	1,114		1,101	

Notes: Entries in rows with variable name labels are least-squares regression coefficients with standard errors in parentheses.

* = p < .05, ** = p < .01, *** = p < .001. All statistical significance tests are two-tailed.

While the findings seem consistent with our theoretical expectations, the fickleness of mediation analyses requires that we thoroughly examine its robustness. We do so by running two robustness checks. First, we tested the fit of the model by replacing the mediating variable with other prospective intervening variables. Alternative causal mechanisms that could theoretically mediate the relationship between exposure to terrorism and support for retaliation include anxiety and perceived threat. We don't hypothesize that either of these variables will intervene since most recent research suggests that anger is the dominant response of civilian populations to terror threats (Wayne 2019), and that the low-information features of cyber attacks is likely to mitigate the influence of perceived threat as a mediator (Egloff 2020). Still, mediation analyses replacing anger with anxiety, and replacing anxiety with threat perception confirm that our model is robust to related variables (see online appendix F for full

analyses).[1] Second, we run a sensitivity analysis to assess whether our mediation is susceptible to a violation of the sequential ignorability principle—that is, whether our mediation results are robust against potentially confounding pre-treatment covariates. The results of this sensitivity analysis (appearing in online appendix F) confirm that the positive ACME findings would require an implausibly large omitted variable to disqualify the positive findings.

Discussion

Terrorism has many faces – the latest of which is digital. In this paper we demonstrate how even a digital form of terrorism - cyber terrorism, can have a considerable impact on public support for retaliatory policies. Empirical research into the effects of cyber terrorism is still in its infancy and the field is characterized by an absence of systematic, methodologically sound data collection and analysis (Dunn Cavelty 2018). This study employed methodologically rigorous analyses of how civilians experience cyber terrorism, and how this influences their policy preferences pertaining to retaliation. Several key findings emerge from these analyses that bear practical contributions to governments' foreign and cyber policies.

First, civilians respond politically to cyber terrorism in the same way as conventional kinetic terrorism, but only when the cyber terror attack results in fatal consequences. To this end, the fatal / non-fatal distinction appears to be the threshold for the onset of strong political effects. This accords with research by Kreps and Das (2017) who identified that the lethality of cyber attacks is a key factor in explaining support for military airstrikes. One way to explain the weak support for retaliation following non-fatal cyber terror attacks is that they may be more associated with cyber-crime. According to this rationale, the absence of fatal consequences and the lack of any immediately identifiable perpetrators cloud the scope and intent of the attack, which is an important indicator in the public's ascription of terrorism (Huff and Kertzer 2017). The need for death and destruction in ascribing a terrorist label to cyber attacks may pose challenges for governments, since there will be diminished public support for activating the full scope of anti-terror tools in response to non-fatal cyber attacks that otherwise meet every definition of terrorism. For example, non-fatal cyber terror attacks that target critical infrastructure - such as electricity stations or financial networks - can cause highly damaging consequences, yet would not be sufficient to arouse public demands for retaliatory strikes in the same way that a conventional attack would.

Second, cyber and conventional terror attacks operate through a similar psychological mechanism with anger as an intervening variable. Having tested for a series of possible intervening variables with similar affect (specifically threat perception and anxiety), we found that only anger succeeded in explaining the pathway by which exposure to terrorism influenced support for retaliatory policies. This pathway held for both conventional and cyber terrorism. The data supports this finding through a robustly tested mediation mechanism, and the fact that the 95% confidence intervals of the average causal mediation effect overlap for both the cyber and conventional models (.052, .15 / .056, .17) indicates that the strength and direction of the model is essentially identical. We acknowledge that even as this resolves some questions, it raises still others. Most striking of these is the question of where feelings of anger are directed in instances of cyber terrorism where attribution is uncertain. We propose that the vicarious retribution theory offers an astute solution to this dilemma, by drawing on social psychological theories to explain how exposure to violence, even in cases where the identity of an attacker is unknown, can still trigger a prosecutorial mindset and a heightened drive for vengeance against ostensibly related targets (Liberman and Skitka 2019; 2017; Washburn and Skitka 2015). While some empirical research has begun to specifically examine how political preferences form when the

[1] Threat perception was measured through a three-item scale that looks at the realistic and symbolic aspects of perceived threat. Each participant was asked whether and to what extent (1 = not at all; 6 = absolutely) a terror attack threatened their and their family's economic situation, personal safety and values. Internal reliability was high.

perpetrator of cyber-attacks is unknown (Jardine and Porter 2020), we encourage additional research to focus on this topic.

Taking account of the comparative foreign policy implications that these finding portends, this study instructs governments interested in pursuing retaliatory strikes following cyber-terror attacks to rouse and emphasize public anger. Likewise governments looking to exercise restraint should attempt to minimize the flame of anger, and rather engage with the public's fear and anxiety. While governments cannot dictate complex societal emotions, especially in the aftermath of crises events, research has indicated that public addresses by leaders can have a significant effect on public anger (Yoo and Jon 2017). The question of inflaming and diminishing anger raises interesting questions about cross-cultural emotional dispositions. Does the renowned stoicism of the British public give the government more flexibility in setting foreign policy in the aftermath of attacks, compared to the perceived emotional volatility of Israelis and Americans (Meyer 2014), whose heightened anger may encourage retaliation? Research in the aftermath of the 7/7 attack in London identified a strategic invocation of British stoicism as a way of minimizing the emotionally laden response to the attacks in a way that offered the government maximum flexibility (Bean, Keränen and Durfy 2011).

A third and unexpected revelation in the data is the country-specific effects. The observed effect of exposure to cyber terrorism on political attitudes was primarily driven by Israeli and United Kingdom respondents, with American respondents showing only minor variation in retaliatory attitudes. Even having selected countries with equivalent levels of susceptibility to cyber terror attacks, similar levels of cyber security preparedness, and comparable levels of civilian fears of terrorism, it appears that there are some country-level variables contributing to differential responses in different countries. One possible explanation for this phenomenon, which is beyond the scope of this particular research, is that Israeli respondents may have more readily available potential perpetrators at the forefront of their minds due to the ongoing conflicts being waged, and so are able to better imagine how and against whom retaliation could take place. Another possible explanation is the national appetite for war and the use of force, which is shaped by core national beliefs about revenge, and which varies across countries (Stein 2015). In Stein's study, the percentage of United Kingdom respondents endorsing revenge was substantially lower than in the United States – reflective of the results in our findings.[2] We encourage future research to probe country-level variables that influence these cyber terrorism models.

We offer two small case studies that illustrate the applicability of this study. In 2020, Israeli authorities announced that they had successfully repelled a sophisticated cyber attack that sought to surreptitiously add chlorine to the country's water supply. The authorities succeeded in resisting the cyber-terror attack, purportedly launched by Iranian-connected attackers, and no casualties were recorded (Heller, 2020). A few years earlier, the United States Department of Homeland Security reported that Russian cyber operatives had successfully infiltrated the control rooms of power plants across the United States – an attack that could have led to significant first- and second-order casualties (Sanger, 2018). In both these cases, the governments sufficed with token and public muted military responses – a far cry from what would surely have been demanded had Russian or Iranian operatives been caught physically entering the critical infrastructure sites. These cases – though far from providing conclusive evidence – offer anecdotal support for our theory that only lethal or destructive cyber-terror attacks will give rise to strong public demands for retaliation, as compared to conventional terrorism that does not possess this conditional threshold.

Myriam Dunn Cavelty's (2007) decade old statement about the scarcity of verified instances of cyber terror attacks causing fatal consequences is still apt. Yet we anticipate that it is but a matter of time until a paradigmatic case is publicly acknowledged. When this does occur, we will need to understand how exposure to cyber terrorism influences political preferences. This study affirms that cyber terrorism can indeed trigger strong public support for retaliatory military action – but only when

[2] Israel was not included in the sample.

the cyber-terror attack causes fatalities. This is a significant finding since it confirms for the first time that the new phenomenon of cyber terrorism can strongly influence support for policy positions. More so, this finding reveals that exposure to cyber terrorism causes different responses to conventional terrorism, validating the need for new and adapted political models for digital forms of terrorism. We also confirm that anger is the key underlying variable bridging the relationship between cyber terrorism and preferences regarding retaliation policies. This extends to the cyber realm the recent trend that views anger as the salient mechanism linking exposure to terrorism with militant preferences.

References

Albahar, M. (2019). Cyber attacks and terrorism: a twenty-first century conundrum. *Science and engineering ethics*, *25*(4), 993-1006.

Applegate, Scott D. 2013. "The dawn of kinetic cyber". *In Cyber Conflict (CyCon), 2013 5th International Conference* (pp. 1-15). IEEE.

Aslam, Faheem, and Hyoung-Goo Kang. 2015. "How different terrorist attacks affect stock markets." *Defence and Peace Economics* 26, no. 6: 634-648.

Backhaus S, Gross ML, Waismel-Manor I, Cohen H and Canetti D (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking*.

Bean H, Keränen L and Durfy M (2011) "This Is London": Cosmopolitan Nationalism and the Discourse of Resilience in the Case of the 7/7 Terrorist Attacks. *Rhetoric & Public Affairs 14*(3), 427-464.

Berrebi, Claude, and Esteban F. Klor. 2008. "Are voters sensitive to terrorism? Direct evidence from the Israeli electorate." *American Political Science Review* 102, no. 3: 279-301.

Bleich, Avraham, Marc Gelkopf, and Zahava Solomon. 2003. "Exposure to terrorism, stress-related mental health symptoms, and coping behaviors among a nationally representative sample in Israel." *Jama* 290, no. 5: 612-620.

Bodenhausen, Galen V., Lori A. Sheppard, and Geoffrey P. Kramer. 1994. "Negative affect and social judgment: The differential impact of anger and sadness." *European Journal of social psychology* 24, no. 1: 45-62.

Bonanno, George A., and John T. Jost. 2006. "Conservative shift among high-exposure survivors of the September 11th terrorist attacks." *Basic and Applied Social Psychology* 28, no. 4: 311-323.

Brenner, Susan W. 2006. "At light speed: Attribution and response to cybercrime / terrorism / warfare." *Journal of Criminal Law & Criminology* 97: 379.

Bulman, May. 2018. "UK more concerned about terror than any other country, finds study." *Independent*, January 8, 2018.

Bumiller, E and Thom S (2012) Panetta Warns of Dire Threat of Cyberattack on U.S. *New York Times,* October 11, 2012.

Canetti, Daphna, Michael Gross, Israel Waismel-Manor, Asaf Levanon, and Hagit Cohen. 2017. "How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks." *Cyberpsychology, Behavior, and Social Networking* 20, no. 2: 72-77.

Canetti-Nisim, Daphna, Gal Ariely, and Eran Halperin. 2008. "Life, pocketbook, or culture: The role of perceived security threats in promoting exclusionist political attitudes toward minorities in Israel." *Political Research Quarterly* 61, no. 1: 90-103.

Canetti, Daphna, Julia Elad-Strenger, Iris Lavi, Dana Guy, and Daniel Bar-Tal. 2017. "Exposure to violence, ethos of conflict, and support for compromise: Surveys in Israel, East Jerusalem, West Bank, and Gaza." *Journal of conflict resolution* 61, no. 1: 84-113.

Carver, Charles S. 2004. "Negative affects deriving from the behavioral approach system." *Emotion* 4, no. 1: 3.

Cavelty, Myriam Dunn. 2007. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Clarke, Richard A. 2016. "The Risk of Cyber War and Cyber Terrorism." *Journal of International Affairs* 70, no. 1: 179-181.

Combs, Cynthia C. 2017. *Terrorism in the twenty-first century*. Routledge.

Critifence. 2018. "2018 Critical Infrastructure Cyber Attack Timeline". Retrieved from: http://www.critifence.com/papers/attack-timeline/files/SCADA%20Cyber%20Attacks%20Timeline

Dorot R (2020) Media Influence Matrix: Israel. CEU Center for Media, Data and Society. Available from: https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/basicpage/1860/mimisraelfunding.pdf (accessed (20 August 2020).

Dunn Cavelty, Myriam. 2018. "Thomas Rid, Cyber War Will Not Take Place." *ERIS–European Review of International Studies* 5, no. 1.

Egloff, Florian J. 2020. Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, *41*, no. 1: 55-81.

Fischer, Agneta H., and Ira J. Roseman. 2007. "Beat them or ban them: The characteristics and social functions of anger and contempt." *Journal of personality and social psychology* 93, no. 1: 103.

Fisk, Kerstin, Jennifer L Merolla and Jennifer M Ramos. 2019. "Emotions, terrorist threat, and drones: Anger drives support for drone strikes." *Journal of Conflict Resolution* 63(4):976-1000.

Foyle, Douglas C. 2004. "Leading the public to war? The influence of American public opinion on the Bush administration's decision to go to war in Iraq." *International Journal of Public Opinion Research* 16, no. 3: 269-294.

Getmansky, Anna, and Thomas Zeitzoff. 2014. "Terrorism and voting: The effect of rocket threat on voting in Israeli elections." *American Political Science Review* 108, no. 3: 588-604.

Gould, Eric D., and Esteban F. Klor. 2010. "Does terrorism work?." *The Quarterly Journal of Economics* 125, no. 4: 1459-1510.

Graves, James, Alessandro Acquisti, and Ross Anderson. 2014. "Experimental measurement of attitudes regarding cybercrime." In *13th Annual Workshop on the Economics of Information Security. Pennsylvania State University*.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2017. "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes." *Journal of Cybersecurity* 3, no. 1: 49-58.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2016. "The psychological effects of cyber terrorism." *Bulletin of the Atomic Scientists* 72, no. 5: 284-291.

Gross, Michael, Daphna Canetti, and Dana Vashdi. 2018. "Cyber Terrorism: Its Effects on Psychological Well-Being, Public Confidence, and Political Attitudes". In Lin H. & Zegart A. (Eds.), Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations (pp. 235-264). Washington, D.C.: Brookings Institution Press.

Haidt, Jonathan et al. 2003. "The moral emotions." *Handbook of Affective Sciences*. 11(2003):852-870.

Halperin, Eran, Alexandra G. Russell, Carol S. Dweck, and James J. Gross. 2011. "Anger, hatred, and the quest for peace: Anger can be constructive in the absence of hatred." *Journal of Conflict Resolution* 55, no. 2: 274-291.

Heller A (2020) Israeli cyber chief: Major attack on water systems thwarted. *Washington Post*. 28 May 2020. https://www.washingtonpost.com/world/middle_east/israeli-cyber-chief-major-attack-on-water-systems-thwarted/2020/05/28/5a923fa0-a0b5-11ea-be06-af5514ee0385_story.html

Herzog, Stephen. 2011. "Revisiting the Estonian cyber attacks: Digital threats and multinational responses." *Journal of Strategic Security* 4, no. 2: 49-60.

Hess, Stephen, and Marvin Kalb (eds). 2003. *The media and the war on terrorism*. Brookings Institution Press, 2003.

Hirsch-Hoefler, Sivan, Daphna Canetti, Carmit Rapaport, and Stevan E. Hobfoll. 2016. "Conflict will harden your heart: Exposure to violence, psychological distress, and peace barriers in Israel and Palestine." *British Journal of Political Science* 46, no. 4: 845-859.

Hua, Jian, Yan Chen, and Xin Robert Luo. 2018. "Are we ready for cyberterrorist attacks? — Examining the role of individual resilience." *Information & Management* 55, no. 7: 928-938.

Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, anxiety, and support of antiterrorism policies." *American journal of political science* 49, no. 3: 593-608.

Huddy, Leonie, Stanley Feldman, Theresa Capelos and Colin Provost. 2002. "The consequences of terrorism: Disentangling the effects of personal and national threat." *Political Psychology* 23(3):485-509.

Huff, Connor and Joshua D. Kertzer. 2017. "People are more likely to describe a violent event as terrorism if the perpetrator is Muslim and has policy goals." *USApp-American Politics and Policy Blog*.

Huff C and Kertzer JD (2018) How the public defines terrorism. *American Journal of Political Science 62*(1), 55-71.

Imai, Kosuke, Luke Keele, Dustin Tingley, and Teppei Yamamoto. 2011. "Unpacking the black box of causality: Learning about causal mechanisms from experimental and observational studies." *American Political Science Review* 105, no. 4: 765-789.

Institute for Economics & Peace. 2017. "Global Terrorism Index: Measuring And Understanding The Impact Of Terrorism (2017)." *Institute for Economics & Peace.* http://economicsandpeace. org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf.

Israel Democracy Institute. 2016. "Peace Index Poll: 1/3 Of Jews Say Jewish Terrorists Should Be Handled Differently Than Palestinian Terrorists" [Press release]. Retrieved June 12, 2019, from https://en.idi.org.il/press-releases/12728

Jaeger, David A., and M. Daniele Paserman. 2008. "The cycle of violence? An empirical analysis of fatalities in the Palestinian-Israeli conflict." *American Economic Review* 98, no. 4: 1591-1604.

Janoff-Bulman, Ronnie, and Ramila Usoof-Thowfeek. 2009. "Shifting moralities: Post-9/11 responses to shattered national assumptions." In *The Impact of 9/11 on Psychology and Education*, pp. 81-96. Palgrave Macmillan, New York.

Jardine, Eric, and Nathaniel D. Porter (2020). Pick Your Poison: The Attribution Paradox in Cyberwar. Retrieved from osf.io/preprints/socarxiv/etb72

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. European Journal of International Security, 2(1), 64-87.

Kertzer, Joshua D. 2017. "Microfoundations in international relations." *Conflict Management and Peace Science*, *34*(1), 81-97.

Klarevas, Louis. 2002. "The "essential domino" of military operations: American public opinion and the use of force." *International Studies Perspectives* 3, no. 4: 417-437.

Kreps, Sarah, and Jacquelyn Schneider. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, *5*(1), tyz007.

Kreps, Sarah, and Debak Das. (2017). Warring from the virtual to the real: Assessing the public's threshold for war over cyber security. Research & Politics, 4(2), 2053168017715930.

Kupatadze, Alexander, and Thomas Zeitzoff. 2019. "In the Shadow of Conflict: How Emotions, Threat Perceptions and Victimization Influence Foreign Policy Attitudes". *British Journal of Political Science*, 1-22.

Lawson ST (2019) *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge.

Lee C, Choi KS, Shandler R, Kayser C (forthcoming) Mapping Global Cyberterror Networks: A Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events. Journal of Contemporary Criminal Justice.

Lerner JS, Gonzalez RM, Small DA and Fischhoff B (2003) Effects of fear and anger on perceived risks of terrorism: A national field experiment. *Psychological science* 14(2), 144-150.

Lewis CW (2000) The Terror that Failed: Public Opinion in the Aftermath of the Bombing in Oklahoma City. *Public Administration Review* 60(3), 201-210.

Liberman P and Skitka LJ (2017) Revenge in US Public Support for War against Iraq. *Public Opinion Quarterly* 81(3), 636-660.

Liberman P and Skitka LJ (2019) Vicarious Retribution in US Public Support for War against Iraq. *Security Studies* 1-27.

Lindsay, Jon R. 2015. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1, no. 1:53-67.

Macdonald S, Jarvis L and Lavis SM (2019) Cyberterrorism Today? Findings From a Follow-on Survey of Researchers. *Studies in Conflict & Terrorism*, 1-26.

Marteau, Theresa M., and Hilary Bekker. 1992. "The development of a six-item short-form of the state scale of the Spielberger State—Trait Anxiety Inventory (STAI)." *British Journal of Clinical Psychology* 31, no. 3: 301-306.

McCarthy J (2016) Americans Cite Cyberterrorism Among Top Three Threats to U.S. *Gallup*. 10 February 2016. https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx

McDermott Rose and Philip G Zimbardo. 2007. "The psychological consequences of terrorist alerts." *In Bongar B, Brown LM, Beutler LE et al. . (eds), Psychology of Terrorism*. Oxford: Oxford University Press, 357–70.

McDermott, Rose. 2010. "Decision making under uncertainty." *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. National Academies Press, Washington, DC: pp. 227–241.

Meyer E (2014) *The culture map: Breaking through the invisible boundaries of global business*. Public Affairs.

Montalvo, Jose G. 2011. "Voting after the bombings: A natural experiment on the effect of terrorist attacks on democratic elections." *Review of Economics and Statistics* 93, no. 4: 1146-1154.

Neria, Yuval, Laura DiGrande, and Ben G. Adams. 2011. "Posttraumatic stress disorder following the September 11, 2001, terrorist attacks: A review of the literature among highly exposed populations." *American Psychologist* 66, no. 6: 429.

Nielsen RK, Schulz A and Fletcher R (2020) The BBC is under scrutiny. Here's what research tells about its role in the UK. *Reuters Institute | University of Oxford*. Available from: https://reutersinstitute.politics.ox.ac.uk/risj-review/bbc-under-scrutiny-heres-what-research-tells-about-its-role-uk (accessed 19 August 2020).

Noguchi M and Ueda H (2019) An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures. *NEC Tech. J. Spec. Issue Cybersecur*ity *12*(2).

Norman J (2018) North Korea, Cyberterrorism Top Threats to U.S. *Gallup*. 5 March 2018. https://news.gallup.com/poll/228437/north-korea-cyberterrorism-top-threats.aspx

Nussio, Enzo. 2020. "Attitudinal and Emotional Consequences of Islamist Terrorism. Evidence from the Berlin Attack." *Political Psychology*, forthcoming.

Pew Research Center (2020) U.S. Media Polarization and the 2020 Election: A Nation Divided. Available from: https://www.journalism.org/2020/01/24/democrats-report-much-higher-levels-of-trust-in-a-number-of-news-sources-than-republicans/

O'Connor, Thomas. 2011. "Definitions, Typologies and Types of Terrorism." Retrieved from: http://www.drtomoconnor.com/3400/3400lect01.htm

Sadler, Melody S., Megan Lineberger, Joshua Correll, and Bernadette Park. 2005. "Emotions, attributions, and policy endorsement in response to the September 11th terrorist attacks." *Basic and Applied Social Psychology* 27, no. 3: 249-258.

Sanger, David E. 2018. "Russian Hackers Appear to Shift Focus to U.S. Power Grid." *New York Times*, July 27, 2018.

Schmitt, Michael N., ed. 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Shafqat, Narmeen, and Ashraf Masood. 2016. "Comparative analysis of various national cyber security strategies." *International Journal of Computer Science and Information Security* 14, no. 1: 129.

Shoshani, Anat, and Michelle Slone. 2008. "The drama of media coverage of terrorism: Emotional and attitudinal impact on the audience." *Studies in Conflict & Terrorism* 31, no. 7: 627-640.

Sinclair, Samuel J., and Daniel Antonius, eds. 2013. *The political psychology of terrorism fears*. Oxford University Press.

Silver, Roxane Cohen, E. Alison Holman, Daniel N. McIntosh, Michael Poulin, and Virginia Gil-Rivas. 2002. "Nationwide longitudinal study of psychological responses to September 11." *Jama* 288, no. 10: 1235-1244.

Sirin, Cigdem V., and Nehemia Geva. 2013. "Examining the distinct effects of emotive triggers on public reactions to international terrorism." *Terrorism and Political Violence* 25, no. 5: 709-733.

Skitka, Linda J, Christopher W Bauman, Nicholas P Aramovich and G Scott Morgan. 2006. "Confrontational and preventative policy responses to terrorism: Anger wants a fight and fear wants "them" to go away." *Basic and Applied Social Psychology* 28(4):375-384.

Small, Deborah A., Jennifer S. Lerner, and Baruch Fischhoff. 2006. "Emotion priming and attributions for terrorism: Americans' reactions in a national field experiment." *Political Psychology* 27, no. 2: 289-298.

Sobel, Richard. 2001. *Impact of Public Opinion on U.S. Foreign Policy Since Vietnam*. New York: Oxford University Press.

Spielberger, Charles D., Eric C. Reheiser, and Sumner J. Sydeman. 1995. "Measuring the experience, expression, and control of anger." *Issues in comprehensive pediatric nursing* 18, no. 3: 207-232.

Spielberger, Charles Donald. 1970. "STAI manual for the state-trait anxiety inventory." *Self-Evaluation Questionnaire*: 1-24.

Spielberger, Charles Donald. 1988. "Manual for the state-trait anger expression scale (STAXI)." *Odessa, FL: Psychological Assessment Resources*.

Steele, Rachel R., Michael T. Parker, and Brian Lickel. 2015. "Bias within because of threat from outside: The effects of an external call for terrorism on anti-Muslim attitudes in the United States." *Social Psychological and Personality Science* 6, no. 2: 193-200.

Stein Rachel M. 2015. "War and revenge: Explaining conflict initiation by democracies." *American Political Science Review* 109(3): 556-73.

Stevens, Daniel, and Nick Vaughan-Williams, N. 2016. "Citizens and security threats: Issues, perceptions and consequences beyond the national frame." *British Journal of Political Science*, *46*(1): 149-175.

Tewksbury D, Jensen J and Coe K (2011) Video news releases and the public: The impact of source labeling on the perceived credibility of television news. *Journal of Communication* 61(2), 328-348.

Tidy J (2020) Police launch homicide inquiry after German hospital hack. *BBC*. 18 September 2020. https://www.bbc.com/news/technology-54204356.

Tomz, Michael, and Jessica LP Weeks. "Public opinion and foreign electoral intervention." *Changes* 2019 (2016): 1.

Valeriano B and Maness RC (2015) Cyber war versus cyber realities: Cyber conflict in the international system. *Oxford University Press, USA*.

Washburn AN and Skitka LJ (2015) Motivated and displaced revenge: Remembering 9/11 suppresses opposition to military intervention in Syria (for some). *Analyses of Social Issues and Public Policy* 15(1), 89-104.

U.S. Army. 2007. "A Military Guide to Terrorism in the Twenty-First Century. Ft. Levinworth, KS: US Army Training and Doctrine Command."

Wayne, Carly. 2019. Risk or Retribution: The Micro-foundations of State Responses to Terror (Doctoral dissertation).

Yoo JW and Jin YJ (2017) The effects of tearful presidential appeals on public anger relief and government reputation. *Corporate Reputation Review 20*(1), 40-56.

White, Jonathan R. 2012. *Terrorism and Homeland Security: Seventh Edition*. Belmont, CA: Wadsworth.